Remarks

This responds to the Office action mailed October 20, 2005 ["the Action"]. Reconsideration of the application is respectfully requested in view of the following remarks. Claims 1-18 are pending in the application. No claims have been allowed. No claims are amended. Claims 1, 2, and 13 are independent.

Rejections Under 35 U.S.C. § 103(a)

The Action rejects claims 1-18 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,772,3321 to Hind et al. ["Hind"] in view of U.S. Patent No. 6,754,829 to Butt et al. ["Butt"]. Applicants respectfully submit the claims in their present form are allowable over the cited art. To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. (MPEP § 2142.)

Hind and Butt do not establish a prima facie case of obviousness for claims 1-18. Accordingly, applicants request that all rejections be withdrawn.

Claim 2

Claim 2 recites, in part,

> *transmitting a trust group membership certificate from the branding device to the security-uninitialized device via the secured network medium, the trust group membership certificate authenticating that the security-uninitialized device is a member of the trust group ....*

[emphasis added]. Claim 2 stands rejected over Hind in view of Butt. The Action alleges that Hind discloses all of Claim 2 except for the language "trust group membership certificate." However, the Action finds this language in Butt. Applicants respectfully disagree.

Butt does not teach or suggest a trust group membership certificate authenticating that a device is a member of a trust group because Butt's disclosure of a session certificate comprising group membership information describes membership information for users, not devices. In its rejection of claim 2, the Action cites to column 3, line 45 to column 4, line 12 of Butt for the proposition that Butt discloses a certificate that "has group membership to access a certain resource."

However, this description mischaracterizes the "group membership" described in Butt. The cited passage describes group membership as follows:

> Generally, *an operator* of a console first authenticates 52 to a core by "logging in" 50 to the core system. This authentication is typically in the form of the operator submitting a username and password pair.... *The core issues 56 the newly created session certificate to the console operator. The session certificate contains special account information for the operator,* based on the operating system of the core. *This information includes the username used to authenticate to the core as well as any of the core's user groups that include this username....*
>
> The console operator can then forward 58 a core-signed session certificate to a manageable device the console operator wishes to manage. *Operator identity and group membership is transmitted to the manageable device inside of the signed session certificate.* This allows a manageable device to conveniently determine access privileges based on operator group data originally in a namespace unknown or foreign to the device.

[Butt, col. 3, line 45 to col. 4, line 12, emphasis added]. The cited section makes clear that the group membership information which is included in Butt's session certificate is information describing an operator. This is supported throughout Butt, and made more clear by Figure 3, which shows an example of a session certificate containing an operator's subject name as well as group membership information, as well as column 8, lines 22-25: "Group membership is simply a way to further describe a console operator ...."

Furthermore Butt explicitly states that "operators" are users, not devices, at column 1, lines 53-55:

> An "operator" is a user or program executing with the credentials of a particular user identity (e.g., a Unix set user-ID (SUID) program).

Thus, the session certificate with group membership information disclosed in Butt cannot teach or describe "a trust group membership certificate authenticating that the security-uninitialized device is a member of the trust group" as recited in claim 2.

Notwithstanding the lack of a "trust group membership certificate" in Butt, there is no motivation to combine Hind and Butt because Hind's teaching of creating individual certificates for each device teaches away from a certificate with group membership information as described in Butt. In its rejection of portions of claim 2 which recite "trust groups" and "trust group membership certificates" the Action cites to column 10, lines 18-29 of Hind. However, Hind does not describe certificates in this passage. Hind's only description of a certificate is in column 9, where Hind describes a certificate which exists solely for the purpose of communication between a central administration server and a device:

> The administration server 1001 then acquires or generates a public/private key pair 1035 *for mobile device 1003*. At 1045 the administration server 1001 puts the created public key 1040 into a certificate request message buffer 1050 *along with device 1003's unique identifier* 1015... and sends 1060 the certificate request 1050 that was prepared for mobile device 1003 to the Certificate authority... When the administration server 1001 receives the signed certificate 1050', *it ... sends the signed certificate 1050' and the corresponding private key ... to the mobile device 1003 over the secure connection 1080 and sends the Certificate Authority's certificate (containing the CA's public key) to mobile device 1003 as well*, and the session is ended.

[Hind, col. 9, lines 32-51; emphasis added]. As the emphasized portions of the passage make clear, the certificate of Hind is device-specific and therefore does not contain group information. In fact, Hind's only allowance for groups describes associating devices with particular groups *after* the certificates have been created:

> *Once a public key, private key and certificate have been created, the administrator can use standard distribution techniques ... to associate the device with a particular user or group of users*, the user or user group or device with access control groups and to log device characteristics of the device.

[Hind, col. 10, lines 18-23; emphasis added]. Thus, Hind requires certificates before association of a device with a group.

Hind teaches two restrictions on certificates: a) the use of certificates only for communication between a central server and a device, and b) certificates are to be established before any group associations are made. These restrictions prevent the use of a certificate which establishes that a device is a member of a trust-group. Applicants note as well that these features of Hind were pointed out in Applicants' Response of July 25, 2005 and that these arguments against Hind were found to be persuasive in the present Action. [Action, page 8, para. 20].

Because Hind's restrictions prevent use of a certificate with group trust membership information, combination of such a reference with Hind would necessarily change the principle of operation of such a reference. Therefore, Hind teaches away from combination with any reference that would show a certificate with group membership information. Because of this, even if Butt were to disclose a trust group membership certificate, there would be no motivation to combine Hind and Butt. Therefore a rejection of claim 2 over a combination of Hind and Butt is improper.

For at least these reasons, there is no motivation to combine Hind and Butt and the combination could not teach or suggest every element of claim 2. Therefore claim 2, and its dependent claims 3-12 are allowable at this time. Applicants request that the rejection of claims 2-12 be withdrawn.

Claim 1

Claim 1 recites, in part:

> *electronically imprinting the security-uninitialized device with group membership and cryptographic key data by the branding device* via the secured network medium ...; and
>
> *initializing the security-uninitialized device to use the cryptographic key data to authenticate group membership of other devices ..., and to provide the security-uninitialized device's group membership to such other devices as authentication that the security-uninitialized device is a member of the trust web,*

[emphasis added]. In its rejection of claim 1, the Action cites only to the sections cited to in its rejection of claim 2. Furthermore, the Action does not address specific language of claim 1, including the above-quoted language which is not found in claim 2. Thus, the Action does not demonstrate how the combination of Hind and Butt teaches or suggests the quoted language of claim 1. For at least this reason, as well as the reasons cited above with respect to claim 2, Hind does not teach or suggest every element of claim 1. Claim 1 is allowable at this time. Applicants request that the rejection of claim 1 be withdrawn.

Claim 13

Claim 13 recites, in part:

> a security resolver operational when initialized with a branding public key to *authenticate trust group membership certificates* provided to the networked

computing device from other devices via the network interface using the branding public key, *and further operational to inhibit interaction via the network interface with other devices not authenticated as in the trust group,...*

[emphasis added]. In its rejection of claim 13, the Action cites only to the sections cited to in its rejection of claim 2. Furthermore, the Action does not address specific language of claim 13, including the above-quoted language which is not found in claim 2. Thus, the Action does not demonstrate how Hind teaches or suggests the quoted language of claim 13. For at least this reason, as well as the reasons cited above with respect to claim 2, Hind does not teach or suggest every element of claim 13. Thus, claim 13, and its dependent claims 14-18, are allowable at this time. Applicants request that the rejection of claims 13-18 be withdrawn.

Conclusion

Claims 1-18 should be allowable. Such action is respectfully requested.

Request for Interview

In view of the preceding amendments and remarks, Applicants believe the application to be allowable. If any issues remain, however, the Examiner is formally requested to contact the undersigned attorney at (503) 226-7391 prior to issuance of the next communication in order to arrange a telephonic interview. This request is being submitted under MPEP § 713.01, which indicates that an interview may be arranged in advance by a written request.

Respectfully submitted,

KLARQUIST SPARKMAN, LLP

One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, Oregon 97204
Telephone: (503) 595-5300
Facsimile: (503) 595-5301

By 
Gregory L. Maurer
Registration No. 43,781